UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,481	03/26/2004	Satoshi Ando	2004-0466A	8335

513 7590 09/12/2007

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
SIKRI, ANISH	

ART UNIT	PAPER NUMBER
2143	

MAIL DATE	DELIVERY MODE
09/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/809,481	ANDO ET AL.	
	Examiner	Art Unit	
	Anish Sikri	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/14/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

The information disclosure statement submitted on 4/14/2005 has been considered by the Examiner and made of record in the application file.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims **1-14** are rejected under 35 U.S.C 102(b) as being unpatentable over Shwed et al (US Pat 5,835,726).

Consider **Claim 1**, Shwed et al discloses an access-controlling method for controlling access of a terminal of an outside network to a server of an inside network using a repeater (Shwed et al, Col 2, Lines 62-67, Col 3 Lines 1-7, 8-29, Col 6 Line 18), the inside network and the outside network being relayed by the repeater (Shwed et al, Col 2, Lines 62-67, Col 3 Lines 1-7, 8-29, Col 6 Line 18), the access-controlling method comprising: permitting transmission of packets sent by the terminal to the server under limited conditions (Shwed et al, Col 2, Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4, Lines 22-43, Col 5, Lines 48-54); changing conditions to generate changed conditions that define packet transmission from the terminal to the server, when the server acknowledges connection between the terminal and the server according to the packets

sent under the limited conditions (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54); and controlling the packet transmission from the terminal to the server under the changed conditions. (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54). Shwed et al clearly shows that a computer device or a gateway can function as a repeater which can be configured for controlling access between external terminal/device outside the internal network to ensure reliable and secure communications can occur.

Consider **Claim 2**, Shwed et al discloses an access-controlling method as defined in claim 1, wherein the limited conditions (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54) limit bandwidth of the packet transmission from the terminal to the server within a predetermined range (Shwed et al, Col 6 Lines 62-67, Col 7 Lines 1-4, Col 17 Lines 55-57). Shwed et al clearly shows on bandwidth can be controlled based on rules and limits placed in the network device.

Consider **Claim 3**, Shwed et al discloses access-controlling method as defined in claim 1, wherein the packets sent under the limited conditions include authentication information to be sent to the server (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54). Shwed et al clearly shows that a computer device or a gateway can function as a repeater which can be configured for controlling access between external terminal/device outside the internal network to ensure reliable and secure communications can occur.

Consider **Claim 4**, Shwed et al discloses access-controlling method as defined in claim 1, wherein said changing conditions further comprises changing conditions of a flow that is defined using an address of the terminal, an port number of the terminal, an address of the server, and a port number of the server (Shwed et al, Col 6 Lines 62-67, Col 7 Lines 1-4, Col 17 Lines 55-57, Col 7 Lines 17-32). Shwed et al clearly shows ports and address is used when communicated between network devices.

Consider **Claim 5**, Shwed et al discloses access-controlling method for controlling access of a terminal of an outside network to a server of an inside network using a repeater (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 6 Lines 18), the inside network and the outside network being relayed by the repeater (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 6 Lines 18), the access-controlling method comprising: receiving encrypted packets from the terminal; decoding the encrypted packets; and notifying access control information concerning the encrypted packets to the repeater (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 6 Lines 18). Shwed et al clearly shows that a computer device or a gateway can function as a repeater which can be configured for controlling access between external terminal/device outside the internal network to ensure reliable and secure communications can occur.

Consider **Claim 6**, Shwed et al discloses access-controlling method as defined in claim 5, wherein the access control information includes information defining a flow concerning the encrypted packets (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 6 Lines 18). Shwed et al clearly shows on the use of encrypting packets when transmission is conducted between network devices located in external and internal network environments.

Consider **Claim 7**, Shwed et al discloses access-controlling method as defined in claim 5, wherein the access control information includes information of an address of the terminal, a port number of the terminal, an address of the server, and a port number of the server (Shwed et al, Col 6 Lines 62-67, Col 7 Lines 1-4, Col 17 Lines 55-57, Col 7 Lines 17-32). Shwed et al clearly shows ports and address is used when communicated between network devices.

Consider **Claim 8**, Shwed et al discloses access-controlling method as defined in claim 1, further comprising: storing access control information in the server; and storing the access control information in the repeater, wherein, when the server changes the access control information, the server notifies the repeater that the access control information has changed (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, 55-67, Col 6 Lines 1-27, 39-54, Col 6 Lines 18). Shwed et al clearly shows on changes to access control in the repeater/network device/gateway are addressed by the server.

Consider **Claim 9**, Shwed et al discloses a repeater for controlling access of a terminal of an outside network to a server of an inside network (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5), and for relaying the inside network and the outside network, the repeater comprising: a first communication unit operable to be connected to the outside network (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5); a second communication unit operable to be connected to the inside network (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54); a storing unit operable to store information correlatively describing a flow concerning packets transmitted via the first communication unit (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, 55-67, Col 6 Lines 1-27, 39-54, Col 6 Lines 18, Col 11 Lines 1-5) and the second communication unit, a bandwidth threshold value of the flow (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54), and a measured bandwidth value of the flow (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5); a classifying unit operable to classify a flow of a packet according to the information defining the flow stored in said storing unit to generate a classified flow (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, 55-67, Col 6 Lines 1-27, 39-54, Col 6 Lines 18, Col 11 Lines 1-5); a measuring unit operable to measure a bandwidth of the classified flow to generate a measured value (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col

4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5), and further operable to store the measured value into said storing unit Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5); a judging unit operable to compare the measured bandwidth of the classified flow with a bandwidth threshold value of the classified flow Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5), to judge whether or not transmission of the flow is acknowledged; and a bandwidth control unit operable to transmit packets belonging to a flow that is judged to be acknowledged by said judging unit Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5), via at least one of the first communication unit and the second communication unit (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5). Shwed et al clearly shows that a computer device or a gateway can function as a repeater which can be configured for controlling access between external terminal/device outside the internal network to ensure reliable, bandwidth controlled and secure communications can occur.

Consider **Claim 10,** Shwed et al discloses repeater as defined in claim 9, wherein the bandwidth threshold value of the flow stored in said storing unit is set a value that limits transmission within a limited range (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5), until the server acknowledges connection between the terminal and the server, and wherein, once the server has acknowledged the connection between the terminal

and the server (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5), the bandwidth threshold value of the flow stored in said storing unit is set another value that limits the transmission more loosely than the limited range (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5). Shwed et al clearly shows that a computer device or a gateway can function as a repeater which can be configured for controlling access between external terminal/device outside the internal network to ensure reliable, bandwidth controlled and secure communications can occur.

Consider **Claim 11**, Shwed et al discloses a server for controlling access with a terminal of an outside network, the server connecting an inside network, the inside network and the outside network being relayed by a repeater (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5), the server comprising: a communication unit operable to be connected to the inside network (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5); a storing unit operable to store information correlatively describing a flow concerning packets transmitted via the communication unit (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5), a bandwidth threshold value of the flow, and a measured bandwidth value of the flow (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5); a classifying unit operable to classify a flow

of a packet according to the information defining the flow stored in said storing unit to generate a classified flow (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5); a measuring unit operable to measure a bandwidth of the classified flow to generate a measured value (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5), and further operable to store the measured value into said storing unit (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5); a judging unit operable to compare the measured bandwidth of the classified flow with a bandwidth threshold value of the classified flow (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5), to judge whether or not transmission of the flow is acknowledged; and a bandwidth control unit operable to transmit packets belonging to a flow that is judged to be acknowledged by said judging unit, via the communication unit (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5). Shwed et al clearly shows that a computer device or a gateway can function as a server which can be configured for controlling access between external terminal/device outside the internal network to ensure reliable, bandwidth controlled and secure communications can occur.

Consider **Claim 12**, Shwed et al discloses a server as defined in claim 11, wherein a value that limits transmission within a limited range is set to the bandwidth threshold value of the flow stored in said storing unit (Shwed et al, Col 2 Lines 62-67,

Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5), until said judging unit judges that transmission between the terminal and the server is acknowledged, and wherein (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5), when said judging unit judges that transmission between the terminal and the server is acknowledged (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5), another value that limits the transmission more loosely than the limited range is set to the bandwidth threshold value of the flow stored in said storing unit (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 11 Lines 1-5). Shwed et al clearly shows that a computer device or a gateway can function as a server which can be configured for controlling access between external terminal/device outside the internal network to ensure reliable, bandwidth controlled and secure communications can occur.

Consider **Claim 13**, Shwed et al discloses a server as defined in claim 11, wherein, when the information stored in said storing unit is changed, said communication unit notifies the repeater that the information stored in said storing unit is changed (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, 55-67, Col 6 Lines 1-27, 39-54, Col 6 Lines 18). Shwed et al clearly shows on how the changes to access control in the storing unit in the repeater/network device/gateway/server are addressed by the server.

Consider **Claim 14,** Shwed et al discloses server as defined in claim 11, further comprising an encryption unit operable to decode an encrypted packet, wherein said communication unit notifies access control information concerning the encrypted packet to the repeater (Shwed et al, Col 2 Lines 62-67, Col 3 Lines 1-7, 8-29, Col 4 Lines 22-43, Col 5 Lines 48-54, Col 6 Lines 39-54, Col 6 Lines 18). Shwed et al clearly shows that a computer device or a gateway can function as a repeater which can be configured for controlling access between external terminal/device outside the internal network to ensure reliable and secure communications can occur.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Anish Sikri whose telephone number is 571-270-1783. The examiner can normally be reached on 8am - 5pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Wiley can be reached on 571-272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Anish Sikri
a.s.

August 27, 2007

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100